In the Claims

Claim 1 (currently amended) A method for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

retrieving ~~the~~ file attributes for ~~the~~ a device file resource used in the system device access attempt;

determining whether the resource that is making the access attempt is a special device file;

searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device; and

generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list.

Claim 2 (original) The method as described in claim 1 further comprising before said searching step the step of terminating said access control method when the accessing resource is not a special device file.

Claim 3 (currently amended) The method as described in claim 1 further comprising after said searching step the step of terminating said access control method when said searching step did not find any database entries that had device specifications that match ~~the~~ device specifications of the special device file making the access attempt.

Claim 4 (currently amended) The method as described in claim 1 wherein said searching step comprises the steps of: retrieving an entry from the mapping database; comparing ~~the~~ device specifications of the special device file making the access attempt to ~~the~~ device specifications of the database entry; and comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 5 (original) The method as described in claim 4 further comprising after said file name comparison step the steps of: generating a device file entry list containing the database entry with the same file specification and file name as the device file making the access attempt; and terminating said searching step.

Claim 6 (currently amended) The method as described in claim 4 further comprising after said file name comparison step the steps of placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 7 (currently amended) The method as described in claim 6 further comprising the steps of:

determining whether there are more entries in the database;

retrieving ~~the~~ a next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and

returning to said special device file comparison step.

Claim 8 (currently amended) The method as described in claim 2 wherein said authorization decision step comprises the steps of:

retrieving the current entry in the special device file entry list;

calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;

determining whether decision component granted access;

determining whether more entries are in ~~this~~ said special device file entry list, if decision component granted access; and

updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 9 (currently amended) The method as described in claim 8 further comprising after said decision determination step the step of denying the access attempt to the system device if the decision component of a special device file entry denies access.

Claim 10 (currently amended) The method as described in claim 8 further comprising the step of allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 11 (original) A method for controlling access to a computing system device being accessed through a device file, said access control being through an externally stored resource and comprising the steps of:

monitoring the computing system for activities related to creating and accessing special device files that represent system devices;

restricting the creation of special device files based on rules defined in the externally stored resource; and

restricting special device file accesses based on rules defined in the externally stored resource.

Claim 12 (currently amended) A computer program product in a computer readable medium for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

instructions for retrieving ~~the~~ file attributes for ~~the~~ a device file resource used in the system device access attempt;

instructions for determining whether the resource that is making the access attempt is a special device file;

instructions for searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a device file entry list of all protected device files that represent said system device; and

instructions for generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list.

Claim 13 (currently amended) The computer program product as described in claim 12 wherein said instructions for searching a mapping database comprise:

instructions for retrieving an entry from the mapping database;

instructions for comparing the device specification of the special device file making the access attempt to the device specification of the database entry; and

instructions for comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 14 (currently amended) The computer program product as described in claim 13 further comprising after said file name comparison instructions: instructions for generating a special device file entry list containing the database entry with the same file specification and file name as the special device file making the access attempt; and instructions for terminating said searching instructions.

Claim 15 (currently amended) The computer program product as described in claim 13 further comprising after said file name comparison instructions the instructions for placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 16 (currently amended) The computer program product described in claim 15 further comprising:

instructions for determining whether there are more entries in the database;

instructions for retrieving the next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and

instructions for returning to said special device file comparison step.

Claim 17 (currently amended) The computer program product as described in claim 12 wherein said authorization instructions comprise:

instructions for retrieving the current entry in the special device file entry list;

instructions for calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;

instructions for determining whether decision component granted access;

instructions for determining whether more entries are in ~~this~~ said special device file entry list, if decision component granted access; and

instructions for updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 18 (original) The computer program product as described in claim 17 further comprising after said decision determination instructions the instructions for denying the access attempt to the system device if the decision component denies access.

Claim 19 (currently amended) The computer program product as described in claim 17 further comprising instructions for allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 20 (original) A computer connectable to a distributed computing system, which includes special device files containing information, related to corresponding system devices comprising:

a processor; a native operating system; application programs;

an externally stored authorization program overlaying said native operating system and augmenting the standard security controls of said native operating system;

a mapping database within said external authorization program containing a system device to a protected object name entries for each protected file system object; and

a decision component within said authorization program for controlling access to special device files representing system devices.

Claim 21 (original) The computer as described in claimed 20 further comprising authorization program for restricting the creation of special device files representing protected system devices.